February 1, 2001

INSPECTOR GENERAL INSTRUCTION 8000.1

SUBJECT: Inspector General Automated Information System (AIS) Management

References: See Appendix A.

A. Purpose. This Instruction updates the Office of the Inspector General, Department of Defense (OIG, DoD), Automated Information System Management.

B. Cancellation. This Instruction supersedes IGDINST 8000.1, *Inspector General Automated Information Systems (AIS) Management,* November 5, 1997.

C. Applicability and Scope. This Instruction applies to the Office of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; Director, Intelligence Review; and the Office of the Deputy General Counsel (Inspector General) (ODGC(IG)), which is provided support by the OIG, DoD. Therefore, this Instruction shall apply to the ODGC (IG) to the extent that the provisions of the Instruction are consistent with this existing arrangement. The ODGC (IG) shall coordinate with the Chief Information Officer (CIO), as necessary, to resolve any issues or questions concerning the applicability of AIS management to the ODGC (IG). For purposes of this Instruction, these organizations are referred to collectively as OIG components.

D. Definitions. See Appendix B.

E. Policy

1. The OIG, DoD, shall have accurate and consistent information available in AISs to effectively enable the execution of its mission. Therefore, the OIG, DoD, shall:

a. Organize and structure data and information to enable interoperability and integration across the OIG, DoD, and related DoD components.

b. Use DoD-wide systems unless OIG, DoD, functioning would be impaired.

c. Base the identification and validation of process improvements on DoD-approved activity models that document functional processes and associated data models that document data and information requirements, including integration of information from other functional areas.

2. The AISs shall be planned, acquired, developed, and implemented from an OIG-wide perspective and in keeping with related DoD-wide initiatives to ensure consistency of information and processes in and across functional areas. Therefore, the OIG, DoD, shall:

a. Use a centrally managed infrastructure for computing, communications, information security, and systems security.

b. Use approved DoD-wide methods, approaches, models, tools, data, information technology, and information services.

c. Achieve integration across component functions, while meeting immediate component-level needs.

3. The OIG, DoD, shall consider security policy throughout the life cycle of an AIS, from the beginning of concept development through design, development, operation, and maintenance until replacement or disposal. The OIG, DoD, shall incorporate Information Security (INFOSEC), into all unclassified and classified AISs. The OIG, DoD, shall consider the following safeguards: physical security, personnel security, need-to-know, administrative security, INFOSEC, and emissions security.

F. Responsibilities

1. The **Inspector General, DoD,** shall:

a. State overall goals, objectives, and priorities for automated information systems management within the OIG, DoD.

b. Serve as the Principal Staff Assistant for those functional areas designated by the Secretary of Defense, including duties associated with AISs.

c. Appoint a CIO and a Designated Approving Authority (DAA).

2. The **Senior Management Group** shall:

a. Resolve, based on analysis provided by the Information Systems Directorate (ISD), Office of the Director of Administration and Information Management (OA&IM), the CIO, and input from other sources, AIS issues requiring executive attention. This includes issues that cross component lines of responsibility, involve significant budget outlays, or involve disagreement as to the best course of OIG, DoD, action.

b. Approve priorities for competing systems and services, including review and approval of acquisitions for information resources, ensuring that acquisition is in accordance with reference a.

3. The **CIO** shall:

a. Serve as the OIG, DoD, advocate for promulgating and implementing the concept of Information Resource Management (IRM), raising awareness of the importance of IRM as integral to meeting mission needs.

b. Provide leadership to improve managing information system resources within the OIG, DoD.

c. Oversee the promulgation of policies and guidance to ensure the most effective and efficient use of information resources.

d. Provide oversight and serve as an expert consultant and central coordinator for the management of all OIG, DoD, IRM activities, including those not related to AISs.

e. Oversee the development, implementation, review, and update of the OIG, DoD, Five-Year Automated Information Resources Management Plan.

f. Oversee and coordinate all agency review activities that fall within the scope of IRM, including security reviews, internal control reviews, and reviews for the General Services Administration (GSA) Triennial Review Program, including those not related to AISs.

g. Ensure that the OIG, DoD, Five Year Automated Information Resources Management Plan is consistent with the budget.

h. Designate a system sponsor for each AIS.

4. The **DAA** shall assume formal responsibility to accept security safeguards prescribed for an information system and is responsible for issuing an accreditation statement that records the decision to accept those as delineated in reference b.

5. The **OIG Component Heads** shall:

a. Develop and maintain on a current basis functional requirements and models of processes for any AIS that affect their component. This shall include ensuring the early and continuous involvement of the DAA to identify security requirements.

b. Designate an Information System Liaison and an alternate to serve as the conduit of information between the ISD and the OIG component for AIS policy, management, and development.

c. Develop cost benefits on any AISs that primarily serve their OIG component.

d. Appoint a component accountable Property Officer and Property Custodians to maintain current accountable property records (e.g., hand receipts, checkout documents) for information resources under their control, in accordance with references c and d.

e. Appoint (if required by reference e) a component Information Systems Security Officer (ISSO) to ensure compliance with AIS security procedures.

f. Communicate their decisions regarding authorized uses of communication systems and non-standard hardware and software to their users.

g. Designate Web Authors to perform duties as delineated in reference c.

6. The **ISD, OA&IM,** shall:

a. Formulate and maintain a coordinated OIG, DoD, Five Year Automated Information Resources Management Plan.

b. Develop AIS policies, standards, and procedures concerned with the technical portion of AISs.

c. Ensure compliance with applicable laws, guidelines, regulations, and standards, both internal and external. This includes, but is not limited to, public laws and OIG, GSA, DoD, and Office of Management and Budget (OMB) directives, instructions, and publications.

d. Manage AIS acquisition, maintenance, and support.

e. Provide information on advances in automation technology.

f. Recommend AIS priorities to the CIO.

g. Provide technical analyses of issues demanding executive attention to the Senior Management Group. These issues include those that cross OIG component lines of responsibility, involve significant budget outlays where there is disagreement as to the best course of OIG, DoD, action, or where it is apparent that deadlines requested by proponent(s) cannot be met.

h. Assist the OIG components in defining functional requirements.

i. Keep the OIG components apprised of the status of any actions that affect their operation.

j. Based on functional requirements provided by the OIG components, define technical solutions consistent with overall OIG, DoD, goals and DoD-wide requirements.

k. Provide end-user support.

l. Develop funding options on AISs with OIG-wide application.

m. Arrange for AIS-related training.

7. The **Administration and Logistics Services Directorate, OA&IM,** shall:

a. Develop policies, standards, and procedures for records, forms, and publications management, which may be involved in an AIS.

b. Develop information systems policies, standards, and procedures relating to references d, f, g, and h. This shall include specifying which electronic documents and data qualify as records.

c. Ensure compliance with applicable laws, guidelines, regulations, and standards, both internal and external. This includes, but is not limited to, public laws and OIG, GSA, DoD, and OMB directives, instructions and publications.

d. Maintain a file of system notices in accordance with reference h.

8. The **Personnel and Security Directorate, OA&IM,** shall:

a. Develop AIS security policies, standards, and procedures.

b. Ensure AIS use complies with applicable security laws, guidelines, regulations, and standards, internal and external. These include, but are not limited to, public laws and OIG (references b, i, and j), GSA, DoD, and OMB publications.

c. Perform duties delegated by the DAA.

d. Advise and assist management on appropriate administrative actions if misuse occurs.

9. The **Information System Liaisons** shall:

a. Ensure that their OIG components are informed of all AIS actions and that the ISD receives component comments by serving as a conduit for timely information between the ISD and their components. This includes being familiar with all AIS-related issues within their components and being able to provide their components' perspective for OIG-wide initiatives as well. This shall

ensure that all the components have input into AISs that will affect them and that the ISD has sufficient information from the components on which to base its decisions.

b. Serve as the review points for any request submitted to the ISD from their OIG components. They also shall ensure that the request is adequately coordinated throughout their OIG component and that all component needs are addressed.

c. Serve as the ISD contact points for processes or functions targeted for automation; act as the OIG components' approval points for phases of the project that require component approval; and assist in the final testing phases on projects before final approval.

d. Serve as members of the Information Systems Liaison Working Group.

10. The **System Sponsor** shall:

a. Issue standard operating procedures for the non-technical portion of the AIS.

b. Ensure the effectiveness and functionality of the portions of the system that do not concern technology or computer programming. This includes, but is not limited to, the accuracy of the data in the system and training on the system's operation.

c. Ensure that the ISD is provided with sufficient information to adequately design and maintain the system.

11. The **End User** shall:

a. Operate information systems only for authorized purposes within established laws, procedures, and guidelines, both internal and external. This includes, but is not limited to, public laws and OIG, GSA, DoD, and OMB directives, instructions, and publications.

b. Ensure the accuracy and integrity of data input, processed, and transmitted.

c. Protect classified and other sensitive information in accordance with references b. h, i, and j.

G. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

/signed/
Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

APPENDIX A
REFERENCES

a. IGDINST 7950.1, *Acquisition of Automated Information System (AIS) Resources*, May 23, 2000

b. IGINST 5200.40, *Security Requirements for Automated Information Systems*, July 20, 2000

c. IGDM 7200.10, *Accountable Property Management Program*, September 30, 1994

d. IGDM 5015.2, *Records Management Program*, June 2000

e. IGDINST 8000.3, *Office of the Inspector General, Department of Defense (OIG, DoD) World Wide Web (Web) Site Administration*, November 22, 1999

f. IGDINST 5400.7, *Inspector General Freedom of Information Act Program*, December 16, 1991, with Change 1

g. Freedom of Information Act, 5 U.S.C. 552, as amended

h. Privacy Act of 1974, 5 U.S.C. 552a, as amended

i. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

j. Computer Security Act 1987, Public Law 100-235

APPENDIX B
DEFINITIONS

a. **Accountable Property Officer** is an individual appointed, in writing, by the proper authority, who maintains item and/or financial records in connection with OIG, DoD, accountable property, irrespective of whether the property is in his/her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use, care, or safekeeping.

b. **Automated Information System (AIS)** is a combination of information, computer, and telecommunications resources and other information technology and personnel resources that collect, record, process, store, communicate, retrieve, and display information.

c. **Automated Information System Management** is the overall management and control of the investment in AISs, including identification and sharing of management information needs; ensuring standardization, control, security, and integrity of data stored or manipulated; and compliance with privacy of records and freedom of information regulations.

d. **Chief Information Officer (CIO)** is the senior official, appointed by the Inspector General, who is responsible for developing and implementing information resources management in ways that enhance OIG, DoD, mission performance through the effective, economic acquisition and use of information. The CIO is currently the Director of the Office of Administration and Information Management.

e. **Communication Systems** include Government-owned telephones, facsimile machines, electronic mail, Internet systems, and commercial systems when use is paid for by the Federal Government.

f. **Component** is a major organizational element reporting directly to the Inspector General.

g. **Database** is a collection of logically related records or files.

h. **Designated Approving Authority (DAA)** is the official, appointed by the Inspector General, who has the authority to decide on accepting the security safeguards prescribed for an information system or that official who may be responsible for issuing an accreditation statement that records the decision to accept these standards. The DAA is currently the Director of the Office of Administration and Information Management.

i. **End-User** is an OIG, DoD, employee or contractor who uses automated equipment to perform work-related tasks.

j. **Function** is appropriate or assigned duties, responsibilities, missions, tasks, powers, or duties of an organizational element.

k. **Functional Requirement** is the definition of an opportunity for improvement and proposal of a more effective or efficient way to perform a task using an AIS detailing what the system should be able to do.

l. **Funding Options** include the type and source of the resources necessary to design and implement an AIS.

m. **Goal** is a desired or needed result to be achieved by the OIG, DoD, over the long term.

n. **Information** is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, maintained in any medium, including but not limited to, computerized data bases, paper, microform, or magnetic tape.

o. **Information Resources** are any combination of hardware, software, and telecommunications, along with the automated and manual procedures necessary to accomplish organizational missions and objectives. Information resources also include the personnel and funds associated with the collection, creation, use, and dissemination of information.

p. **Information System** is the organized collection, processing, transmission, and dissemination of information according to defined procedures, whether automated or manual. It includes people, equipment, and policies.

q. **Information Security (INFOSEC)** is a composite of means to protect telecommunications systems and AISs, and the information they process.

r. **Information Systems Security Officer (ISSO)** is the person who ensures compliance with AIS security procedures at the operations site or installation.

s. **Mission** is a comprehensive description of the scope and purpose of the OIG, DoD, and its components. It specifies what the OIG, DoD, business is and what it should be.

t. **Network Security Manager (NSM)** is responsible for the overall security operation of the network and oversees policy, guidance, and assistance in network security matters. In addition, the NSM ensures that the network complies with the requirements for interconnecting to external systems.

u. **OIG Environment** is any computer, media, or network used by the OIG, DoD.

v. **Property Custodian** is an individual appointed in writing, by proper authority, to exercise proper custody, care, and safekeeping of OIG, DoD, accountable property entrusted to his or her possession or under his or her supervision. He or she may incur pecuniary liability for losses because of failure to exercise his or her obligation.

w. **Support** includes diagnosing and resolving problems regarding operating and using standard OIG, DoD, hardware, software, telecommunications, and software applications.

x. **System** is a collection of people, equipment, policies, and methods organized to accomplish an activity.

y. **System Sponsor** is the designated proponent or main user of an AIS. The CIO shall designate a sponsor for each AIS. In most cases, this will be the OIG component that has major responsibility for the process most affected by the AIS.

z. **Web Author** is the person who develops, publishes, and maintains Internet and Intranet content.